Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U001704

Особливі позначки: відкрита

Дата реєстрації: 14-05-2025

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Каптьол Євгеній Юрійович
2. Yevhenii Kaptol

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0001-8612-2196

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Кібербезпека

Дата захисту:

Спеціальність за освітою: Безпека інформаційних і комунікаційних систем

Місце роботи здобувача: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 8459

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.54.02, 20.54.04, 20.56.01

Тема дисертації:

1. Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу

2. Methods for evaluation and comparative analysis of asymmetric electronic signatures resistant to classical and quantum cryptanalysis

Реферат:

1. Дисертаційна робота присвячена розв’язанню актуальної задачі: аналізу та дослідженню, оцінці та порівнянню існуючих та перспективних квантовостійких електронних підписів по сукупності безумовних, умовних та прагматичних критеріїв. Мета і завдання дослідження. Обгрунтування вибору, аналіз та дослідження, оцінка та порівняння існуючих та перспективних квантовостійких електронних підписів по сукупності безумовних, умовних та прагматичних критеріїв. У першому розділі дисертації (Аналіз стану безпеки існуючих та обгрунтування вимог до методів перспективних квантовостійких електронних підписів) на основі пошуку джерел, що присвячені обгрунтуванню вимог та моделей безпеки вирішуються задачі

визначення стану розвитку квантових технологій та вимог до асиметричних електронних підписів на міжнародному та національному рівнях. Проблеми захищеності від нового класу квантових атак виникли декілька десятиліть тому. На основі рішень та аналізу від наукової спільноти (професорів Менезис та Кобліц та інших) NIST США оголосив конкурс на розроблення проектів стандартів квантовостійких асиметричних кпритоперетворень, в тому числі, ЕП. В наступні роки відбулось три раунди і в 2022 році на форумі NIST США конференція прийняла рішення про стандартизацію і в NIST 8413 наведено перелік стандартизованих ЕП. В подальшому після річного дослідження у США були прийняті федеральні стандарти FIPS 203 на основі Crystal-Kyber, FIPS 204 на основі Crystall-Delithium та FIPS 205 на основі геш-функції. Щодо математичного методу Falcon продовжено дослідження його безпечності. На національному рівні було прийнято рішення взяти за основу математичні методи Crystall-Delithium, Crystal-Kyber, Falcon та ЕП на основі одноразових ключів. Крім того, було оголошено продовження досліджень на 4-му раунді та було організовано конкурс на розроблення альтернативних варіантів електронного підпису. Аналіз показав, що з'явилось багато пропозицій на переших раундах конкурсів: 69 на першому конкурсі та 40 на конкурсі альтернативних варіантів ЕП. Таким чином поряд з розробкою квантовостійких ЕП і виникла проблемна задача розроблення методичних основ оцінки та порівняння асиметричних криптоперетворень, в тому числі ЕП. Вирішення як теоретичної так і практичної задачі дозволило на основі математичних решіток розробити та прийняти квантовостійкі ЕП ДСТУ 9212:2023 та протокол АСШ та інкапсуляції ключів ДСТУ 8961:2019. У другому розділі дисертації (Модель безпеки та критерії оцінки і порівняння перспективних постквантових електронних підписів) обгрунтовано моделі порушника, загроз та безпеки. Показано, що асиметричні електронні підписи мають множину різноманітних застосувань, котрі висувають дещо відмінні один від одного вимоги до криптографічних перетворень типу асиметричний електронний підпис. Наведено переліки безумовних, умовних та прагматичних критеріїв. У третьому розділі дисертації (Науково-методичні основи розробки, оцінки та порівняння існуючих та перспективних квантовостійких електронних підписів за безумовними, умовними та прагматичними критеріями) обгрунтовано комплексну методику оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу. Запропоновано вдосконалення комплексної методики оцінки та порівняльного аналізу в частині врахування в процесі оцінки та порівняння за прагматичними критеріями мети здійснення порівняння та можливих варіантів застосування ЕП, що призодить до збільшення точності та відповідності отриманого результату вихідним вимогам. У четвертому розділі дисертації (Аналіз, оцінка та порівняння існуючих та кандидатів на перспективні квантовостійкі національні та міжнародні електронні підписи за безумовними критеріями) здійснено оцінку та порівняльний аналіз як кандидатів на стандартизацію між собою, так і вже стандартизованих для використання в перехідний та пост-квантовий періоди алгоритми електронного підпису між собою. Проведено порівняння отриманих результатів порівняння вже стандартизованих алгоритмів з міжнародними результатами. У п'ятому розділі дисертації (Програмне моделювання та експериментальні дослідження процесів порівняння за безумовними критеріями) уточнено оцінки та отримано експерементальні результати порівняння електронних підписів за допомогою розробленого програмного забезпечення. Для електронного підпису Falcon запропонована атака відновлення ключів та досліджено вплив використання фіксованої точки замість плаваючої точки в процесі формування підпису на безпеку.

2. The dissertation work is devoted to the solution of the actual problem: analysis and research, evaluation and comparison of existing and promising quantum-resistant electronic signatures according to a set of unconditional, conditional and pragmatic criteria. The purpose and tasks of the research. Justification of the choice, analysis and research, evaluation and comparison of existing and prospective quantum-resistant electronic signatures according to a set of unconditional, conditional and pragmatic criteria. In the first chapter of the dissertation (Analysis of the security status of existing and justification of requirements for methods of promising quantum-resistant electronic signatures) based on the search for sources devoted to the justification of requirements and security models, the tasks of determining the state of development of quantum technologies and requirements for asymmetric electronic signatures at the international and national levels are solved. The problems of security

against a new class of quantum attacks arose several decades ago. Based on the decisions and analysis of the scientific community (Professors Menezes and Koblitz and others), the US NIST announced a competition for the development of draft standards for quantum-resistant asymmetric cryptographic transformations, including ES. In the following years, three rounds took place, and in 2022, at the NIST USA forum, the conference made a decision on standardization and a list of standardized ES is given in NIST 8413. Subsequently, after a year of research, the US federal standards FIPS 203 based on Crystal-Kyber, FIPS 204 based on Crystall-Delithium, and FIPS 205 based on a hash function were adopted. Regarding the Falcon mathematical method, research into its security continued. At the national level, it was decided to take as a basis the mathematical methods of Crystall-Delithium, Crystal-Kyber, Falcon and ES based on one-time keys. The analysis showed that many proposals appeared in the previous rounds of competitions: 69 in the first tender and 40 in the tender of alternative ES. Thus, along with the development of quantum-resistant ES, the problematic task of developing methodical bases for evaluating and comparing asymmetric cryptotransformations, including ES, arose. The solution of both theoretical and practical problems made it possible to develop and adopt quantum-resistant ES DSTU 9212:2023 and the ASSH protocol and key encapsulation DSTU 8961:2019 on the basis of mathematical lattices. In the second chapter of the dissertation (Security model and criteria for evaluating and comparing promising post-quantum electronic signatures), the models of the intruder, threats and security are substantiated. It is shown that asymmetric electronic signatures have a variety of applications, which put forward somewhat different requirements for cryptographic transformations of the asymmetric electronic signature type. Lists of unconditional, conditional and pragmatic criteria are given. In the third chapter of the dissertation (Scientific and methodological foundations of the development, evaluation and comparison of existing and promising quantum-resistant electronic signatures according to unconditional, conditional and pragmatic criteria), a comprehensive methodology for the evaluation and comparative analysis of asymmetric electronic signatures resistant to classical and quantum cryptanalysis is substantiated. An improvement of the comprehensive methodology for the evaluation and comparative analysis is proposed in terms of taking into account in the process of evaluation and comparison according to pragmatic criteria the purpose of the comparison and possible options for the application of the ES, which will contribute to increasing the accuracy and compliance of the obtained result with the initial requirements. In the fourth chapter of the dissertation (Analysis, evaluation and comparison of existing and candidates for promising quantum-resistant national and international electronic signatures according to unconditional criteria), an evaluation and comparative analysis of both candidates for standardization among themselves and already standardized for use in the transitional and post-quantum periods electronic signature algorithms among themselves is carried out. The obtained results of the comparison of already standardized algorithms with international results were compared. In the fifth chapter of the dissertation (Software modeling and experimental studies of comparison processes by unconditional criteria), the estimates are refined and experimental results of the comparison of electronic signatures are obtained using the developed software. For the Falcon electronic signature, a key recovery attack is proposed and the impact of using a fixed point instead of a floating point in the signature formation process on security is investigated.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Potii, O., Kachko, O., Kandii, S., & Kaptol, Y. (2024). Determining the effect of a floating point on the Falcon digital signature algorithm security. Eastern-European Journal of Enterprise Technologies, 1(9 (127), 52–59. (Scopus, Web of Science) https://journals.uran.ua/eejet/article/view/295160/291714 DOI: 10.15587/1729-

4061.2024.295160.
- Kachko, O., Gorbenko, Y., Kandii, S., & Kaptol, Y. (2024). Improving protection of falcon electronic signature software implementations against attacks based on floating point noise. Eastern-European Journal of Enterprise Technologies, 4(9 (130), 6–17. (Scopus, Web of Science) https://journals.uran.ua/eejet/article/view/310521 DOI: 10.15587/1729-4061.2024.310521.
- Kaptiol, Y. Y. (2022). Analysis of the RAINBOW post-quantum electronic signature algorithm state and attacks on it for the period of the NIST PQC third round completion. Radiotekhnika, 2(209), 87–92. http://rt.nure.ua/article/view/262495/258911 DOI: 10.30837/rt.2022.2.209.09.
- Yu.I. Gorbenko, M.V. Yesina, V.A. Ponomar, I.D. Gorbenko, E.Yu. Kapt'ol Scientific and methodological bases of analysis, evaluation and results of comparison of existing and promising (post-quantum) asymmetric cryptographic primitives of electronic signature, protocols of asymmetric encryption and key encapsulation protocols. Radiotekhnika. 2023. 212, 42-66. http://rt.nure.ua/article/view/286512/280398 DOI: 10.30837/rt.2023.1.212.05.
- Є. Ю. Каптьол, І. Д. Горбенко. Аналіз можливостей та особливості програмування задач криптології на квантовому комп'ютері. Radiotekhnika, 202, 37-48. http://rt.nure.ua/article/view/215822/215989 DOI: 10.30837/rt.2020.3.202.03.
- Gorbenko, I., & Kaptol, Y. (2023). Analysis and comparison of the security of electronic signatures based on new quantum-resistant problems. Radiotekhnika, 4(215), 31–45. http://rt.nure.ua/article/view/299724/292240 DOI: 10.30837/rt.2023.4.215.04.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Горбенко Іван Дмитрович
2. Ivan Gorbenko

Кваліфікація: д. т. н., професор, 05.13.21

Ідентифікатор ORCID ID: 0009-0003-6979-8946

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Корченко Олександр Григорович
2. Oleksandr Korchenko

Кваліфікація: д. т. н., професор, 05.13.21

Ідентифікатор ORCID ID: 0000-0003-3376-0631

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

Власне Прізвище Ім'я По-батькові:

1. Толюпа Сергій Васильович
2. Serhii Toliupa

Кваліфікація: д. т. н., професор, 05.12.02

Ідентифікатор ORCID ID: 0000-0002-1919-9174

Додаткова інформація:

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, буд. 60, Київ, 01033, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Сектор науки: Університетський

Власне Прізвище Ім'я По-батькові:

1. Чевардін Владислав Євгенович
2. Vladyslav Chevardin

Кваліфікація: д. т. н., професор, 05.13.21

Ідентифікатор ORCID ID: 0000-0002-1070-4568

Додаткова інформація:

Повне найменування юридичної особи: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Код за ЄДРПОУ: 24978555

Місцезнаходження: вул. Московська, буд. 45/1, Київ, 01011, Україна

Форма власності: Державна

Сфера управління: Міністерство оборони України

Ідентифікатор ROR:

Сектор науки: Університетський

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Олійников Роман Васльович
2. Roman Oliynykov

Кваліфікація: д. т. н., професор, 05.13.05

Ідентифікатор ORCID ID: 0000-0002-3494-0493

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Сектор науки: Університетський

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Єсін Віталій Іванович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Єсін Віталій Іванович
Відповідальний за підготовку облікових документів	Шевченко Андрій Олександрович
Реєстратор	УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна